Credential Management

Robert D. Olson

June 11, 2004

Overview

- General security overview
- Some PKI history
- Validation
- Authorization
- Operational Issues
- Certificate Authorities
- Management tools

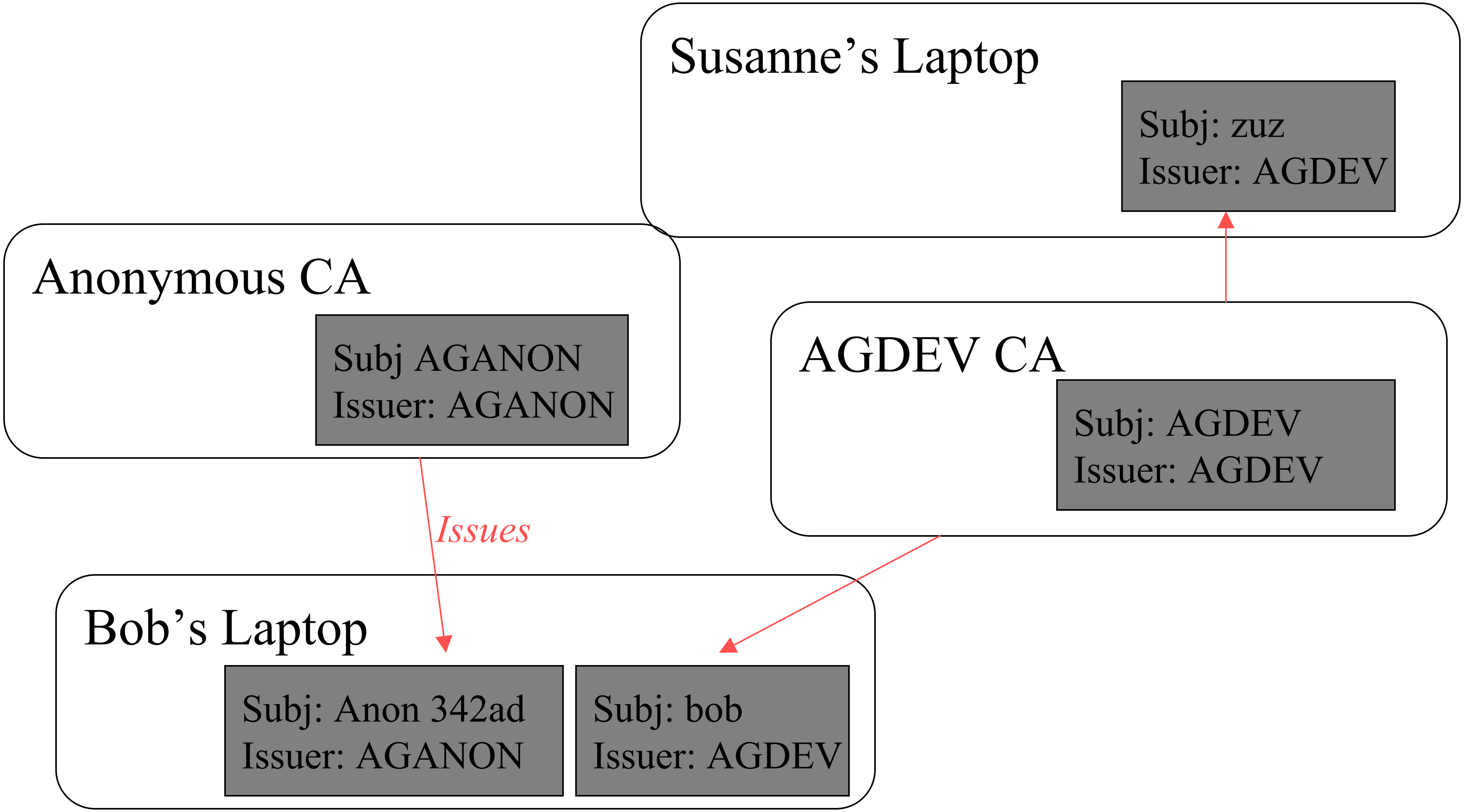
Security Overview

- AG Toolkit provides foundation for secure communication
- Essential component: Authentication
- Process by which a claimed identity is verified
- AG needs authentication for …
  - Users
  - Services
  - Devices

State of the Toolkit

- Given the preceding discussion, how does this affect the AG Toolkit?
  - Any communicating party must have an identity certificate.
  - Any communicating party must hold the trusted CA certificate for the CA that issued certificates to any party with which it communicates.

Certificate Distribution



Susanne's Laptop

Subj: zuz
Issuer: AGDEV

Anonymous CA

Subj AGANON
Issuer: AGANON

AGDEV CA

Subj: AGDEV
Issuer: AGDEV

Issues

Bob's Laptop

Subj: Anon 342ad
Issuer: AGANON

Subj: bob
Issuer: AGDEV

Identity Certificates

- Each “human” user of the AG required to have identity certificate
- (“Required” is actually a result of the policy enforced by a particular service)
- ANL AG group provides two mechanisms for obtaining identity certificates

AGDev CA

- FuturesLab group runs a fairly casual Certificate Authority
- Requests generated through the AG Venue Client
- Issuing policy requires real names and email addresses
- Generated certificates installed through the AG Venue Client as well

Anonymous CA

- For testing purposes, and for instances when a more serious identity is not required
- An “online CA”, certificates issued immediately by an online service
- Names always of the form “Anonymous User XXXXX”

Service Certificates

- Autonomous services (VenueServer, node services, etc) also require identity certificates
- Typically do not have encrypted private keys (protection via OS security)
- As of AG2.2, AGDev CA also issues service certificates

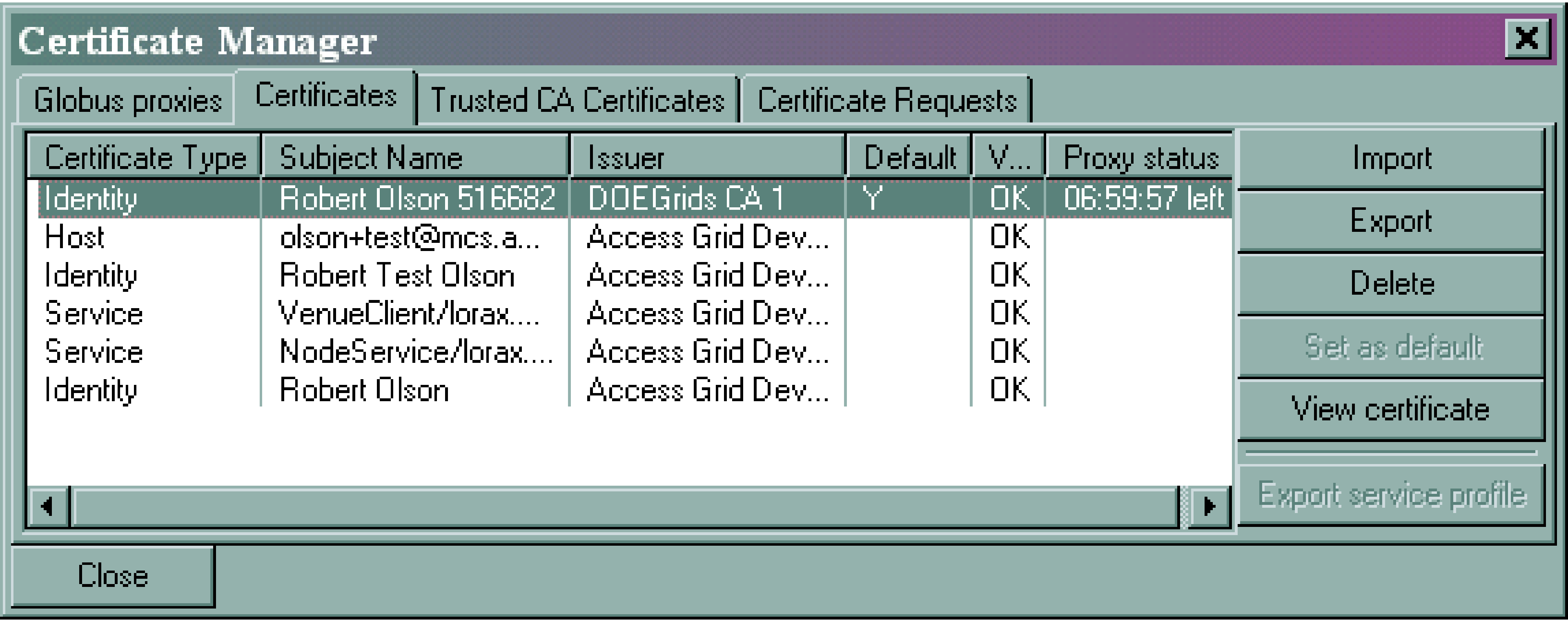
Other Certificate Authorities

- An organization that has an existing PKI may use this easily with AG
- Existing CA certificates to be imported to all participating AG software (clients and services)
- Identity certificates imported for use
- Future enhancements to aid in the determination of precisely which CA a client or service requires

Certificate Management in AG Toolkit

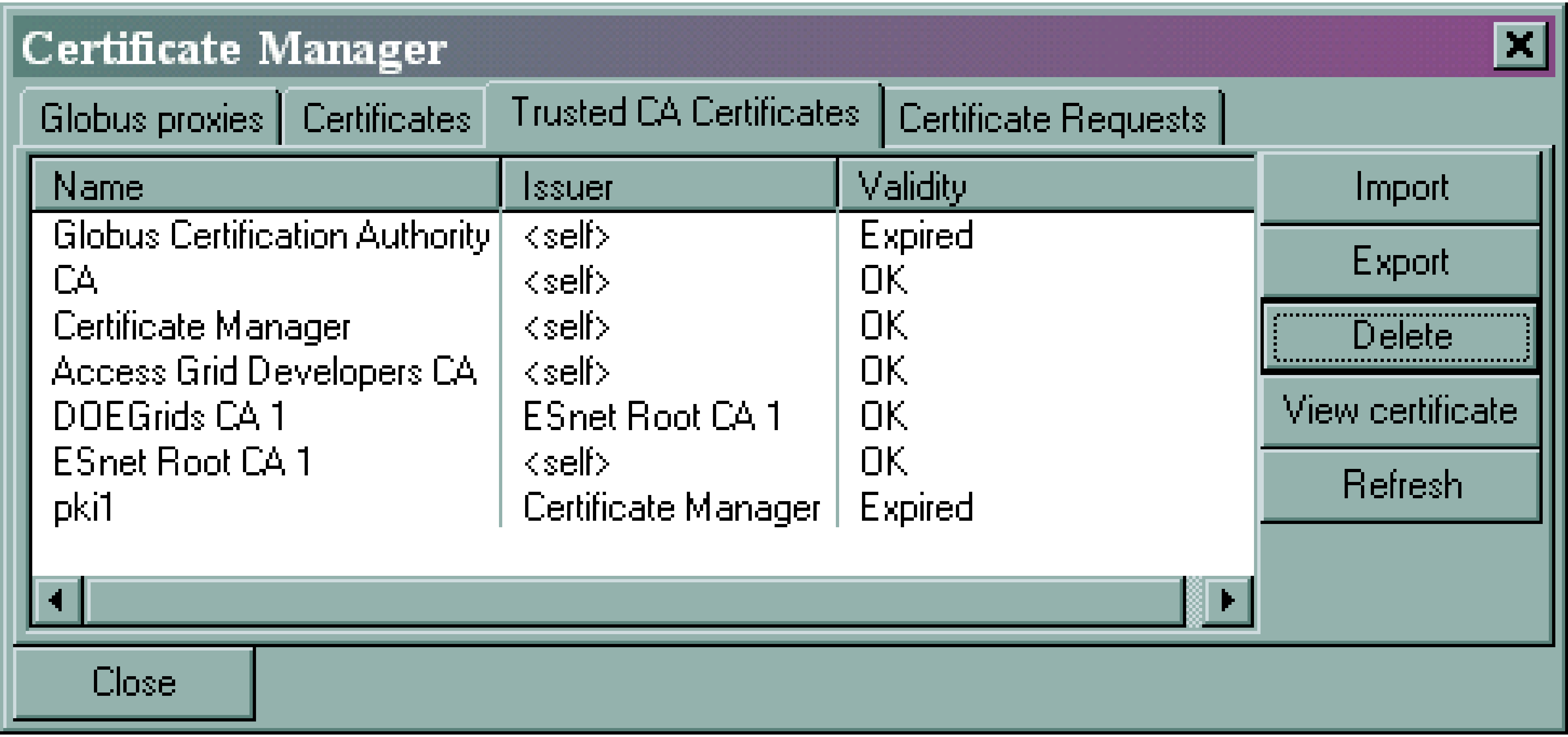
- AGTk provides comprehensive certificate management tools
  - Certificate Manager and Repository objects for use by applications
    - Maintain sets of identity, CA, proxy certificates
    - Provides interface to underlying security environment
  - Command-line and GUI-based interfaces for manipulating certificates
- Security tools entirely hide the details from application code

GUI Certificate Manager
Certificate View



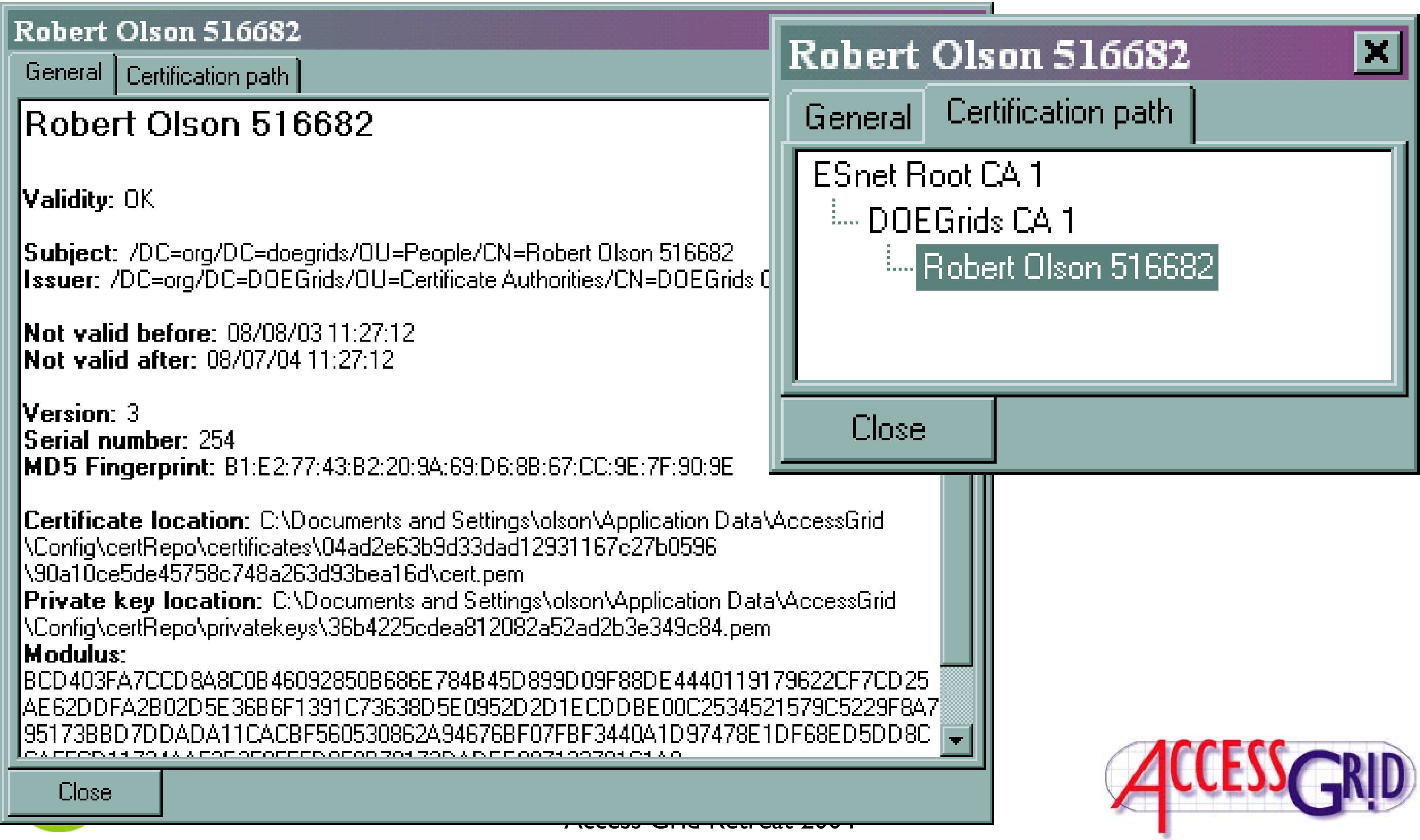
Certificate Type	Subject Name	Issuer	Default	V...	Proxy status
Identity	Robert Olson 516682	DOEGrids CA 1	Y	OK	06:59:57 left
Host	olson+test@mcs.a...	Access Grid Dev...		OK	
Identity	Robert Test Olson	Access Grid Dev...		OK	
Service	VenueClient/lorax....	Access Grid Dev...		OK	
Service	NodeService/lorax....	Access Grid Dev...		OK	
Identity	Robert Olson	Access Grid Dev...		OK	

GUI Certificate Manager
Trusted CA Certificates



Name	Issuer	Validity
Globus Certification Authority	<self>	Expired
CA	<self>	OK
Certificate Manager	<self>	OK
Access Grid Developers CA	<self>	OK
DOEGrids CA 1	ESnet Root CA 1	OK
ESnet Root CA 1	<self>	OK
pki1	Certificate Manager	Expired

GUI Certificate Manager
Certificate Detail



Robert Olson 516682

Validity: OK

Subject: /DC=org/DC=doegrids/OU=People/CN=Robert Olson 516682
Issuer: /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids C

Not valid before: 08/08/03 11:27:12
Not valid after: 08/07/04 11:27:12

Version: 3
Serial number: 254
MD5 Fingerprint: B1:E2:77:43:B2:20:9A:69:D6:8B:67:CC:9E:7F:90:9E

Certificate location: C:\Documents and Settings\olson\Application Data\AccessGrid
\Config\certRepo\certificates\04ad2e63b9d33dad12931167c27b0596
\90a10ce5de45758c748a263d93bea16d\cert.pem
Private key location: C:\Documents and Settings\olson\Application Data\AccessGrid
\Config\certRepo\privatekeys\36b4225cdea812082a52ad2b3e349c84.pem
Modulus:
BCD403FA7CCD8A8C0B46092850B686E784B45D899D09F88DE44401191796 22CF7CD25
AE62DDFA2B02D5E36B6F1391C73638D5E0952D2D1ECDDBE00C2534521579C5229F8A7
95173BBD7DDADA11CACBF560530862A94676BF07FBF3440A1D97478E1DF68ED5DD8C

Robert Olson 516682

General | Certification path

ESnet Root CA 1
- DOEGrids CA 1
  - Robert Olson 516682

Future Directions

- Toward easier certificate management
- Toward easier installation
- Toward support for future Web Services

Other Certificate Access Mechanisms

- Burdensome to copy identity certificates about from machine to machine
- Potential solutions:
  - Memory stick (works with current tech)
  - Encryption tokens (requires new support from Globus Tookit)
  - Certificate proxying servers (MyProxy)

Node Cluster Services

- In a multiple-machine node, each component requires a cert
- However, if components do not communicate externally, do not need outside CA
- Local CA set up at install time, certs issued to all node components
- If remote access required (remote control), user identity certs may be issued by the node administrator (tight control of outside access possible)

Insecure Toolkit

- In some environments, security may not matter at all
- Toolkit supports the use of entirely insecure communications
- No certificates required
- All messaging in the clear
- Appropriate for closed networks
  - – I worry about compromise potential on the open Internet

Graduated Security

- We've discussed tightly locked-down systems, and unlocked systems…
- Is there a happy medium?
- Consider that:
  - For most use, we don't need bulletproof security
  - But for some applications, and in some communities, we do
  - We may desire to shift from one mode to another dynamically

Graduated Security, cont.

- Consider the *Pervasive Collaborative Computing Environment Project* (Deb Agarwal, LBNL)
- Among other things, PCCE is investigating a graduated security model
  - Supports varying levels of user registration
  - Varying modes of user authentication and credentials
- Supports both established and ad hoc collaborative modes
- Research question: How can this be applied to the AG?

Graduated Security, Cont.

- Anonymous Certificates also a intermediate solution
- Anon cert uniquely identifies a client, but does not bind user identity to the client identity
- Certs issued automatically (And immediately)

Online CA with external authenticators

- Automated CA which issues certificate based on some external criteria
- Example: Unix login authenticator
  - User submits cert request with NIS login & password (encrypted)
  - CA uses NIS to perform password verification
  - On success, CA issues certificate
- To the user, he used his Unix login to gain access to resource
- To the resource, the user provided a valid certificate

Web Services

- Grid-based computing moving toward Web Services for high-level communication
- SOAP + WSDL + high level Web Service interface
  - WS-Resource – resource management
  - WS-Service Group – service registry
  - WS-Security – secure communications

WS-Security

- SOAP enhancements for
  - Message integrity
  - Message confidentiality
  - Single-message authentication
  - Encoding of security tokens
- As WS technology matures, AG project will track the security work
- Likely to still utilize X509 PKI, retaining utility of Certificate Management tools

Linkage to other projects

- Depending on user requirements, and based on our support of the Globus PKI mechanisms, possible to support such things as the NMI-supported tools:
  - Kerberos-based authentication, via KX509
  - SAML/Shibboleth for interaction with web-based single sign-on systems

Credits

This work is supported in part by:

- The Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, Office of Science, U.S. Department of Energy, under Contract W-31-109-ENG-38, the National Science Foundation under Grant No. ANI-0222509,
- Support from Microsoft Research, and
- Federal funds from the National Library of Medicine, National Institutes of Health, under Contract No. N01-LM-3-3508 and Grant R01-LM-06756,

And viewers like you.